APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,971	10/06/2003	Robert M. Best	493-37-3	4769

996   7590   08/02/2007
GRAYBEAL, JACKSON, HALEY LLP
155 - 108TH AVENUE NE
SUITE 350
BELLEVUE, WA 98004-5973

EXAMINER
SAN JUAN, MARTINJERIKO P

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
08/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *26 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) ~~1-108~~ 90-108 is/are pending in the application.

    4a) Of the above claim(s) ~~1-89~~ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *90-108* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 April 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date *6/01/2004, 1/30/2004*.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

This is a response to Applicant's Amendments filed on April 17, 2007.

Claims 1-89 were originally pending.

Claims 1-89 were rejected on the first action filed on February 9, 2007.

Applicant has cancelled claims 1-89, added new claims 90-108, and amended

Specifications and Drawings.

Claims 90-108 are now pending in the application.

Specification

1. The Substitute Specification and Drawings filed on April 26, 2007 has been entered

and accepted. Applicant deleted matter regarding an embodiment about game software

(programs and data) distribution on an optical disk or in a memory cartridge with a built-

in secondary cryptoprocessor, together with an encrypted key for decrypting the

encrypted software. This remaining subject matter contained in the Substitute

Specification is still supported in the Original Specification filed on October 6, 2003.

2. The Substitute Specification filed on April 26, 2007 is objected to under 35

U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a)

states that no amendment shall introduce new matter into the disclosure of the

invention. The added material which is not supported by the original disclosure is as
follows:

a.   Editing the 2nd sentence of Par 0069 of the Original Specification

regarding "Cryptoprocessor 52 may should be attached to the motherboard..." is

introducing new matter with regards to claims 93, and 103.

Applicant is required to cancel the new matter in the reply to this Office Action.

Response to Arguments

Applicant's arguments with respect to claims 1-89 have been considered but are

moot because applicant cancelled claims 1-89 in view of the new claims 90-108.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

1.   Claim 90, and 100 are rejected under 35 U.S.C. 112, second paragraph, as

being indefinite for failing to particularly point out and distinctly claim the subject matter

which applicant regards as the invention.

Regarding claims 90 and 100, the phrase "substantially" renders the claim

indefinite because it is unclear whether the limitation(s) following the phrase are part of

the claimed invention. See MPEP § 2173.05(d).

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2.   Claims 93, and 103 are rejected under 35 U.S.C. 112, first paragraph, as failing

to comply with the written description requirement. The claim(s) contains subject matter

which was not described in the specification in such a way as to reasonably convey to

one skilled in the relevant art that the inventor(s), at the time the application was filed,

had possession of the claimed invention.

      a.   Regarding claims 93, and 103, the closest support from the specification

would have been an embodiment described in paragraphs [0085-0089] of the

Substitute Specification with regards to Figure 4. The disclosed embodiment is

based on 2 cryptoprocessor chips. Also, the said cryptoprocessor chip that these

claims are referring to is the primary cryptoprocessor chip [Fig 4 (new drawings),

Itm 52] located in the game console's mainboard performing the

encryption/decryption and part execution, instead of the secondary

cryptoprocessor [Fig 4 (new drawings), Itm 303] located in the memory cartridge

whose function is to provide a "matched" chip ID securely with the retailer.

Editing the 2nd sentence of Par 0069 of the Original Specification regarding

"Cryptoprocessor 52 may ~~should~~ be attached to the motherboard..." is

introducing this new matter.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459

(1966), that are applied for establishing a background for determining obviousness

under 35 U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating obviousness or nonobviousness.

1.   Claims 90-108 are rejected under 35 U.S.C. 103(a) as being unpatentable over

previously cited prior art Ishibashi et al. [US PN 6728379 B1], and further in view of

McCarty [US PN 5666411].

Regarding claim 90, Ishibashi et al. teach a method of securely distributing content data

for processing in a single-chip secure cryptoprocessor comprising: encrypting in a

network server a first program [US PN 6728379 B1, Col 1, Ln 20 – Content data include

further works, eg. program.] under control of a first encryption key [US PN 6728379 B1,

Col 4, Ln 34-35 – content encryption key for encryption of content data]; transmitting

said encrypted first program from said server to said cryptoprocessor [US PN 6728379

B1, Col 5, Ln 19-21 – transmit encrypted content data to user-side information

processor]; encrypting a decryption key corresponding to said first encryption key to

produce at least one encrypted data block [US PN 6728379 B1, Col 5, Ln 16 – generate

an encrypted content decryption key]; transmitting said data block to said

cryptoprocessor chip [US PN 6728379 B1, Col 5, Ln 18-21]; (g-mod) decrypting said

encrypted data block in said cryptoprocessor chip to produce a decrypted said

decryption key in said cryptoprocessor chip; decrypting said encrypted first program in

said cryptoprocessor chip under control of said decryption key to produce decrypted

content program [US PN 6728379 B1, Col 10, Ln 52-53].

Ishibashi et al. do not teach: encrypting said unique identifier in said cryptoprocessor

chip to produce an encrypted identifier; transmitting said encrypted identifier to said

server; re-encrypting in said server said unique identifier together with a decryption key

corresponding to said first encryption key to produce at least one encrypted data block;

decrypting said encrypted data block in said cryptoprocessor chip to produce a

decrypted identifier and said decryption key in said cryptoprocessor chip; decrypting

said encrypted first program in said cryptoprocessor chip under control of said

decryption key to produce executable digital instructions stored in said program

memory; and executing said digital instructions in said processor core in said

cryptoprocessor chip to generate output data if said decrypted identifier has a

predetermined relationship with said unique identifier in said cryptoprocessor chip.

Moreover, Ishibashi et al does not explicitly teach a program of executable instructions.

McCarty teaches a method of securely distributing program of instructions for execution

in a single-chip secure cryptoprocessor that contains substantially unique identifier data

that distinguishes different cryptoprocessor units, encryption circuitry for encrypting said

identifier, decryption circuitry for decrypting encrypted digital program instructions,

writable program memory for storing decrypted instructions, and processor core for

executing said decrypted instructions which are inaccessible from said secure

cryptoprocessor chip from locations outside of said chip after fabrication of said chip is

completed [US PN 5666411, Col 7, Ln 30-33]; the method comprising: transmitting said

identifier to said server [US PN 56664111, Col 10, Ln 62-66 -- It is inherent that the

new chip identifier is transmitted in order to receive appropriate upgrade data for the

new client processor.]; receiving a data block in said cryptoprocessor chip to produce an

identifier in said cryptoprocessor chip [US PN 56664111, Col 10, Ln 62-66]; decrypting

said encrypted first program in said cryptoprocessor chip under control of a decryption

key to produce executable digital instructions stored in said program memory [US PN

5666411, Col 11, Ln 10-25] [US PN 5666411, Col 12, Ln 26-30]; and executing said

digital instructions in said processor core in said cryptoprocessor chip to generate

output data if said server identifier has a predetermined relationship with said unique

identifier in said cryptoprocessor chip [US PN 56664111, Col 10, Ln 62-66 – The data

block contains upgrade data comprising the DEVID – Ed(SYSKEY) which is the new

system key encrypted under the Device (chip) key corresponding to a Device (chip) ID.]

[US PN 56664111, Col 11, Ln 25-35 – Execution of instructions in said cryptoprocessor

is evidenced by the Cryptofunction calls.].

It would have been obvious to one of ordinary skill in the art at the time of invention to

extend Ishibashi's et al. program content data to include program executable

instructions or software. The suggestion/motivation for extending digital content to

include software would be to protect proprietary software from disclosure and

unauthorized use, and to enforce license limits on number of users of the software [US

PN 6728379 B1, Ln 13-40] in the market of electronic software distribution.

Also, it would have been obvious to one of ordinary skill in the art at the time of

invention to replace the cryptoprocessor machine of Ishibashi et al. with the

cryptoprossesor machine of McCarty thus extending the user/client side computer

instruction set architectures [US 5666411, Col 4, Ln 61-67]. The suggestion/motivation

for combining would have been to prevent content piracy by also controlling the method

of execution of the protected content program by McCarty's cryptoprocessor [US

5666411, Col 4, Ln 23-46].

Also it would have been obvious to one of ordinary skill in the art at the time of invention

to encrypt said unique identifier of McCarty's cryptoprocessor to be transmitted to the

server, just as taught by Ishibashi et al. when encrypting charge information data by a

common session key to be transmitted to the server [US 6728379 B1, Col 7, Ln 48-51].
As such, the server would also obviously re-encrypt said unique identifier (contained in
the upgrade data of McCarty) along with other data sent back to the user/client side
such as the content decryption key, which would then have to be decrypted by the
cryptoprocessor upon reciept. The suggestion/motivation would have been to protect
data while being transmitted to another party and to minimize/simplify data packet
transmissions.

Ishibashi et al. and McCarty are analogous art because they are both in the same field
of protecting digital content. Therefore, it would have been obvious to combine the
inventions of Ishibashi et al., and McCarty.

Regarding claim 91, the combined inventions of Ishibashi et al. and McCarty teach the
method of claim 90, further comprising the steps of: generating a session key in said
server [US 6728379 B1, Col 7, Ln 39]; encrypting said unique identifier in said
cryptoprocessor chip under control of said session key to produce said encrypted
identifier; and decrypting said encrypted identifier in said server under control of said
session key to produce a decrypted identifier.
The combined invention of Ishibashi et al. and McCarty does not explicitly teach:
transmitting said session key in encrypted form to said cryptoprocessor; decrypting said
encrypted session key in said cryptoprocessor chip to produce a decrypted session key.

Nevertheless, it would have been obvious to transmit said session key in encrypted form to said cryptoprocessor; and decrypting said encrypted session key in said cryptoprocessor chip to produce a decrypted session key. While there are various protocols/methods in establishing symmetric keys by two parties in the art, it is also common in the art just to encrypt and transmit such encrypted symmetric key.

Regarding claim 92, the combined invention of Ishibashi et al. and McCarty is essentially a general purpose machine [US PN 5666411, Col 4, Ln 62-67], and as such, a video game system is inherent and would teach all the limitations wherein said cryptoprocessor chip is a component in a video game system and said output data generated by said cryptoprocessor is game data that is processed by a graphics co-processor in said game system that generates graphics data for display on a display device.

Regarding claim 93, the combined invention of Ishibashi et al. and McCarty inherently teaches wherein said cryptoprocessor chip is a component in a manually removable memory device [US PN 6728379 B1, Col 6, Ln 50 – PC Card] for use in a video game system [inherent in a general purpose type machine] and it is inherent that said output data generated by said cryptoprocessor is game data that is processed by a graphics co-processor in said game system that generates graphics data for display on a display device.

If the combined invention does not explicity teach the method, wherein said

cryptoprocessor chip is a component in a manually removable memory device for use in

a video game system. It still would have been obvious to modify the combined

invention to have the cryptoprocessor chip as a component in a manually removable

memory device for use in a video game system since it is common in the art for

computers to have different kinds of removable hardware modules. The

suggestion/motivation for modifying would have been for the ease of physically securing

the cryptoprocessor chip module, or for ease of upgradeability and maintenance of the

computer machine.

Regarding claim 94, the combined invention of Ishibashi et al. and McCarty teach the

method of claim 90, wherein said cryptoprocessor chip is a component in a computer

and said output data generated by said cryptoprocessor is address data that identifies

memory locations of non-encrypted program instructions [US PN 5666411, Col 13, Ln

5-39] executed by a second processor in said computer [Second processor can be

graphics co-processor, device I/O controller processor, and etc. which is inherent.].

Claim 95 is rejected because the combined invention of Ishibashi et al. and McCarty

teaches the methods of claims 90 and 93.

Regarding claim 96, the combined invention of Ishibashi et al. and McCarty does not

explicitly teach wherein said cryptoprocessor chip communicates with a second

processor through a data transmission path that comprises wireless transmission. It would have been obvious to modify the combined invention to have the cryptoprocessor chip communicate with a second processor through a data transmission path that comprises wireless transmission since it is common in the art for computers to have different kinds of wireless input devices such as a mouse, keyboard, joysticks, etc. that inherently has a processor. The suggestion/motivation for modifying would have been for the ease of use such wireless devices.

Regarding claim 97, the combined invention of Ishibashi et al. and McCarty teach the methods of claim 90, wherein said cryptoprocessor chip inhibits output of said executable digital instructions from said data memory to a location outside of said secure cryptoprocessor chip [US PN 5666411, Col 13, Ln 5-28 – The Zone Management Record process inherently has the capability of inhibiting output of said executable digital instructions from said data memory to a location outside of said secure cryptoprocessor chip.].

Regarding claim 98, it would be inherent that the combined invention of Ishibashi et al. and McCarty would teach the method of claim 90 wherein said output data generated by said cryptoprocessor contain instructions that are executed by a second processor because various computer devices and modules contain processors (said secondary processor) that has to receive instructions, routines, sub-routines, data, information for their respective devices in order to run any kind of software.

Regarding claim 99, the combined invention of Ishibashi et al. and McCarty would teach

the method of claim 90, further comprising the step of downloading said encrypted first

program of executable digital instructions and said encrypted data block through a

retailer computer [US PN 6728379 B1, Fig 8, Itm 10,20 – Content Provider/Network

Service Provider].

Claim 100 and 102 are rejected using the same references and rationale as claim 90

because it is the apparatus performing the method of claim 90.

Claim 101 is rejected using the same references and rationale as claim 98 and

generation of secondary data for processing by said cryptoprocessor chip is inherent

because there is constant communication/dialogue between cryptoprocessor and other

computer devices (containing said secondary processor).

Claim 103 is rejected using the same references and rationale as claim 95 because it is

the apparatus performing the method of claim 95.

Claim 104 is rejected is rejected because it is the same processor performing the

methods of claim 90.

Claim 105 is rejected using the same references and rationale of claim 96 because it is

still the same cryptoprocessor.

Claim 106 and 107 are rejected using the same references and rationale of claim 90

because the cryptoprocessor is the same chip of claim 104, wherein said output data is

processed by a second processor in a computer which has an architecture of a general

purpose machine.

Claim 108 is rejected using the same references and rationale as claim 90 since the

cryptoprocessor chip of claim 90 implements an EEPROM [US PN 56664111, Col 7, Ln

56] which is a type of non-volatile writable memory.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

US PN 6704871 B1 to Kaplan et al. – Discloses a general purpose cryptographic

co-processor.

Applicant's amendment or new claims necessitated the new ground(s) of rejection

presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See

MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in
37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE
MONTHS from the mailing date of this action. In the event a first reply is filed within
TWO MONTHS of the mailing date of this final action and the advisory action is not
mailed until after the end of the THREE-MONTH shortened statutory period, then the
shortened statutory period will expire on the date the advisory action is mailed, and any
extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of
the advisory action. In no event, however, will the statutory period for reply expire later
than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the
examiner should be directed to Martin Jeriko P. San Juan whose telephone number is
571-272-7875. The examiner can normally be reached on M-F. 8:30a - 6:00p EST.
If attempts to reach the examiner by telephone are unsuccessful, the examiner's
supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number
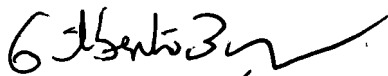for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO

Customer Service Representative or access to the automated information system, call

800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/

Martin Jeriko San Juan

Examiner. Art Unit 2132

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100